

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИСТОРИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра документоведения

ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

*Методические рекомендации
для студентов дневного отделения по специальности
«Организация и технология защиты информации»*

Составитель Л.Н. Устина

Самара
Издательство «Универс групп»
2006

*Печатается по решению Редакционно-издательского совета
Самарского государственного университета*

Рецензент

к.п.н., доц. кафедры документных коммуникаций СГАКИ Т.Ф. Дыченко

Научный редактор

д-р. ист. наук, проф. Ю.Н. Смирнов

Защита и обработка конфиденциальных документов : методические рекомендации для студентов дневного отделения по специальности «Организация и технология защиты информации» / сост. Л.Н. Устина. – Самара: Изд-во «Универс групп», 2006. – 24 с.

© Устина Л.Н., составление, 2006

© Самарский государственный университет, 2006

СОДЕРЖАНИЕ

Пояснительная записка	4
Содержание курса	6
Тематика лабораторных занятий	11
Темы рефератов	17
Вопросы к экзамену	19
Список источников и литературы по всему курсу	21

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс «Защита и обработка конфиденциальных документов» предназначен для студентов, обучающихся по специальности «Организация и технология защиты информации» и входит в цикл дисциплин

Целью курса является изучение комплекса проблем безопасности конфиденциальной документированной информации и направлений деятельности, построения и функционирования правовых, организационных, технических и технологических процессов, обеспечивающих защиту конфиденциальных документов на стадии составления, исполнения, хранения.

Задачи дисциплины:

- овладение теоретическими, практическими и методическими вопросами безопасности конфиденциальной документированной информации;
- освоение методов защиты документированной предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения;
- анализ приемов работы с документированной конфиденциальной информацией на традиционных и электронных носителях;

1.2. Требования к уровню подготовки студента, завершившего изучение данной дисциплины

Студенты, завершившие изучение данной дисциплины, должны знать:

- законодательные и нормативные основы реализации защиты документированной конфиденциальной информации;
- направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к конфиденциальной документированной информации, ее утраты;
- функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов;
- направления и методы работы с персоналом, обладающим конфиденциальной информацией; методику изучения профессиональных, деловых, личных и моральных качеств претендентов на должности; методику обучения, инструктирования сотрудников;
- разрешительную систему доступа, критерии и способы доступа персонала к тайне фирмы, информационным системам;
- методы охраны помещений, предназначенных для хранения конфиденциальной документации и действия персонала по сбережению доку-

ментации в обычных и экстремальных ситуациях, проведения охранных мероприятий;

- методику защиты информации при проведении основных деловых мероприятий (переговоры, прием посетителей), в рекламной и выставочной деятельности, работе кадровой службы и др.;

- порядок оборудования помещений, выделенных для работы с конфиденциальной информацией, аттестации помещений;

- особенности документирования организационно-правового обеспечения функционирования систем защиты информации, служб безопасности, организации работы персонала.

В соответствии с учебным планом очного обучения курс приходится на 6 и 7 семестры и состоит из 68 лекционных и 32 часов лабораторных занятий.

Лабораторные занятия проводятся по темам курса, требующим приобретения практических навыков работы с документами, закрепления теоретических знаний, полученных на лекциях и в результате самостоятельной работы над учебным материалом. Часть тем выполняется на ПЭВМ.

СОДЕРЖАНИЕ КУРСА

ВВЕДЕНИЕ.

РАЗДЕЛ 1. Организационно-правовые основы обеспечения информационной безопасности.

Тема 1.1. Концептуальные основы информационной безопасности в Российской Федерации, необходимость организации защиты конфиденциальной документированной информации. Документирование информации как обязательное условие включения информации в информационные ресурсы. Критерии ценности информационных ресурсов. Понятие государственной тайны. Виды недобросовестной конкуренции. Промышленный и экономический шпионаж.

Тема 1.2. Роль и место информационных ресурсов ограниченного доступа. Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в дореволюционной России. Классификация конфиденциальной информации. Предпринимательская (коммерческая) тайна как форма защиты деловой и производственной информации. Служебная тайна. Профессиональная тайна. Тайны личная и семейная. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной.

Понятие конфиденциального документа. Общая классификация конфиденциальных документов. Сроки (период) конфиденциальности.

Тема 1.3. Источники конфиденциальной информации и каналы ее утраты. Классификация источников конфиденциальной документированной информации. Характеристика каждого источника. Классификация каналов объективного распространения конфиденциальной информации. Уязвимость информации. Интерес к информации как предпосылка возникновения угроз. Понятия угрозы информации, виды угроз.

Понятие несанкционированного канала утраты документированной информации. Случайные и преднамеренные условия возникновения такого канала. Последствия образования канала несанкционированного доступа к информации: утрата носителя и конфиденциальности информации, разрушение информации, ее кража, модификация, подмена, фальсификация и др. Отличие разглашения и утечки информации. Технические каналы утечки конфиденциальной информации. Комплексность использования организационных и технических каналов. Легальные и нелегальные способы получения ценной и конфиденциальной информации о физических и юридических лицах. Понятие злоумышленника, постороннего и случайного лица.

РАЗДЕЛ 2. Принципы и структура системы защиты информации

Тема 2.1. Разработка перечня сведений, составляющих конфиденциальную информацию. Цели и задачи перечня сведений, составляющих коммерческую тайну. Состав сведений, которые не могут быть тайной. Классификация ценной информации в предпринимательских структурах различного типа. Принципы определения состава ценных сведений, подлежащих защите в конкретной фирме. Перечни списочные и проблемно-ориентированные. Организационные формы составления и ведения перечня. Методики сбора, анализа и обобщения сведений. Место маркетингового исследования в процедуре разработки перечня. Разграничение уровня конфиденциальности сведений, определение срока конфиденциальности, регламентация места документирования, использования и хранения, состава сотрудников, которым эти сведения необходимы по работе. Ведение перечня на ЭВМ.

Тема 2.2. Доступ персонала к конфиденциальным сведениям, документам и базам данных. Цели и задачи разрешительной системы доступа персонала и иных лиц к конфиденциальным сведениям, документам, базам данным и продукции. Структура разрешительной системы и ее связь с требованиями деловой целесообразности и персональной ответственности руководителей и сотрудников за сохранности тайны фирмы. Оформление разрешения о допуске сотрудника к конфиденциальным документам фирмы. Ответственность должностного лица за выданное разрешение. Иерархичность процедуры доступа.

Формы письменной индивидуальной регламентации разрешения на доступ – резолюции, перечни, списки, матрицы, схемы и т.п. Порядок доступа к конфиденциальным сведениям представителей других фирм и служащих государственных учреждений.

Тема 2.3. Нормативно-методические документы по организации системы защиты информации. Регламентация права коммерческой структуры на защиту своей тайны. Регламентация технологии защиты информации от потенциальных и реальных угроз. Регламентация технологии обработки, движения и хранения конфиденциальных документов на традиционных и технических носителях. Регламентация технологии работы персонала фирмы с документами, вычислительной и организационной техникой, средствами связи. Регламентация работы с персоналом. Регламентация системы охраны фирмы. Регламентация защиты информации в экстремальных ситуациях. Состав методических указаний, правил, памяток, схем и наглядных пособий.

РАЗДЕЛ 3. Защищенный документооборот

Тема 3.1. Понятие, принципы, цели и задачи защищенного документооборота как совокупности документопотоков. Критерии безопасности документооборота. Типовая структура технологических стадий входного, выходного и внутреннего потоков конфиденциальных документов. Принципиальная взаимосвязь документопотока и применяемой технологической системы обработки и хранения документов. Организационные и технологические требования к обработке и хранению конфиденциальных документов.

Тема 3.2. Учет конфиденциальных документов. Угрозы документам в процессе учета, способы их защиты. Цели и задачи учета конфиденциальных документов и носителей конфиденциальной информации. Виды учета. Функции и структура традиционного справочно-информационного банка данных по документам (журналов учета, контрольных журналов, карточек). Автоматизированный учет бумажных и электронных конфиденциальных документов. Применение электронной подписи при получении документа. Назначение и процедуры учета поступивших конфиденциальных документов. Назначение и процедуры учета подготовленных конфиденциальных документов. Назначение и процедуры учета конфиденциальных документов выделенного хранения. Инвентарный учет документов. Учет носителей конфиденциальной информации. Учет законченных производством дел, картотек и журналов учета.

Тема 3.3. Документирование конфиденциальной информации. Угрозы информации при документировании. Принципы документирования конфиденциальной информации. Этапы подготовки конфиденциальных документов. Определение уровня грифа конфиденциальности. Виды грифов и ограничительных отметок, порядок их оформления. Изменение и снятие грифа конфиденциальности. Предварительный учет бумажных и технических носителей информации. Виды носителей. Маркировка носителей. Особенности составления черновика конфиденциального документа. Изготовление оригинала документа. Формы учета проектов подготовленных документов. Порядок уничтожения черновиков и проектов. Особенности согласования, подписания и утверждения конфиденциальных документов. Порядок копирования и тиражирования конфиденциальных документов. Особенности пакетирования отправляемых документов, доставки их адресатам.

Тема 3.4. Организация работы персонала с конфиденциальными документами. Угрозы документам в процессе работы с ними руководителей, специалистов и технических сотрудников фирмы. Особенности процедуры рассмотрения документов руководителем. Ознакомление исполнителей с документами и передача документов на исполнение. Получение докумен-

тов от исполнителей. Учет документов, находящихся у исполнителей. Порядок хранения документов на рабочем столе. Хранение документов в нерабочее время. Порядок работы с конфиденциальными документами в командировках.

Тема 3.5. Формирование конфиденциальных документов в дела, хранение дел и передача их в архив. Уничтожение документов, дел и носителей информации. Особенности процедуры составления, ведения и закрытия номенклатуры дел. Особенности оформления дела при его заведении, формировании и закрытии. Экспертиза ценности конфиденциальных документов. Составление описи дел, передаваемых в архив фирмы (ведомственном архиве). Классификация и учет архивных дел, научно-справочный аппарат, организация использования документов и дел. Процедура составления акта об уничтожении конфиденциальных документов и дел. Особенности физического уничтожения документов.

Назначение, задачи и типы проверок наличия конфиденциальных документов, дел и носителей информации. Методика ведения проверки. Состав проверяемых документов при квартальной проверке. Процедура проверки правильности работы исполнителей с конфиденциальными документами. Состав проверяемых документов при годовой проверке наличия документов. Основания и порядок проведения нерегламентированной проверки наличия.

РАЗДЕЛ 4. Особенности работы персонала с недокументированной конфиденциальной информацией.

Тема 4.1. Организация подбора персонала для работы с конфиденциальной информацией. Роль кадровой работы в защите предпринимательства. Угрозы безопасности информации, исходящие от персонала и направления ее защиты. Психологические особенности человека, владеющего тайной. Особенности приема сотрудников на работу, связанную с владением конфиденциальной информацией. Принципы, этапы и методы отбора персонала. Состав и анализ документов, получаемых от кандидата. Организация собеседования, анкетирования, тестирования и опроса. Критерии отбора кандидатов на должность. Формы обязательств о неразглашении тайны фирмы. Особенности содержательной части трудового контракта.

Тема 4.2. Организация работы с персоналом, обладающим конфиденциальной информацией. Классификация сотрудников по степени их владения тайной фирмы и объемам известной им конфиденциальной информации. Направления и методы работы с каждой из выделенных категорий. Организация и методика обучения сотрудников правилам обеспечения безопасности информации. Проведение инструктирования. Формы и методы индивидуальной работы. Поведение персонала в экстремальных ситуациях. Порядок проведения служебного расследования по фактам разгла-

шения или утечки информации, утраты носителей и документов. Формы морального и материального стимулирования сотрудников. Фонд экономического стимулирования. Гибкие формы заработной платы. Премии и штрафы. Роль психологического климата в воспитании ответственного отношения в работе. Правовая ответственность персонала за разглашение конфиденциальной информации. Особенности увольнения сотрудников с работы. Соблюдение работниками деловой этики.

Тема 4.2. Порядок проведения совещаний и переговоров по конфиденциальным вопросам, приема посетителей. Угрозы безопасности информации в процессе проведения совещаний и переговоров. Общие требования к отбору информации для оглашения. Виды совещаний и переговоров. Документирование информации, оформление стенограмм, протоколов и итоговых документов. Порядок использования аудио- и видеозаписи. Инженерно-технические требования к помещениям, их охране. Обязанности участников совещаний, переговоров и лиц, ответственных за их проведение. Классификация посетителей. Обязанности лиц, ответственных за прием посетителей. Методы контроля поведения посетителей. Требования к помещениям для приема посетителей.

Тема 4.3. Защита документированной информации в процессе публикаторской, рекламной и выставочной деятельности. Угрозы безопасности информации в процессе публикаторской, рекламной и выставочной деятельности. Методы анализа ценности информации, предложенной для широкого доступа, методы защиты ценных элементов идеи. Виды публикаторской деятельности, оформление разрешения фирмы на публикацию. Виды рекламной деятельности, особенности отражения информации в рекламной продукции. Оформление разрешения фирмы на издание рекламной продукции. Виды выставочной деятельности и презентаций продукции. Методы подготовки стендистов по вопросам защиты ценной информации. Контроль эффективности защиты информации в публикаторской, рекламной и выставочной деятельности.

ТЕМАТИКА ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Занятие 1-2.

Цель – по текстам Законов «О Государственной тайне» и «О коммерческой тайне», а также по статьям Уголовного кодекса РФ определить виды документов, содержащих соответствующие виды тайн, классифицировать их по группам.

Задание. Определить меру ответственности за нарушение требований к защите информации.

Источники

Уголовный кодекс РФ. Ст. 272-276, 283, 284, 325.

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»

Закон РФ от 21.07.93 № 5485-1 «О государственной тайне» (в ред. от 29.06.2004).

Указ Президента РФ от 30.11.95 № 1203 «О перечне сведений, отнесенных к государственной тайне» (в ред. от 29.05.2002).

Федеральный закон от 03.04.95 № 40-ФЗ «О федеральной службе безопасности в Российской Федерации».

Федеральный закон от 12.08.95 № 144-ФЗ «Об оперативно-розыскной деятельности».

Федеральный закон от 31.05.96 № 61-ФЗ «Об обороне» (в ред. от 22.08.2004)

Федеральный закон от 10.01.96 № 5-ФЗ «О внешней разведке» (в ред. от 22.08.2004).

Закон РФ от 05.03.92 № 2446-1 «О безопасности» (в ред. от 25.07.2002).

Закон РФ от 11.02.92 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» (в ред. от 10.01.2003).

Литература

Корольков А.В. Актуальные направления научных исследований по обеспечению информационной безопасности структур государственной службы Российской Федерации // Проблемы информатизации. – 2001. – № 1.

Белов В.П. Информационная достаточность и информационная безопасность в государственном управлении // Проблемы информатизации. – 2001. – № 1.

Занятие 3-4.

Цель работы – проанализировать информационные ресурсы, предприятия, выявить исходные данные для оценки системы информационной безопасности предприятия

Задание.

1. Составить приказ о создании комиссии из ведущих специалистов фирмы, экспертов и менеджеров для анализа имеющихся информационных ресурсов

2. Составить перечень вопросов (не менее 50) для руководства фирмы для выявления ценных и конфиденциальных сведений фирмы.

В результате опроса должны быть выявлены:

организационная структура фирмы;

функции руководителей, руководителей подразделений, руководителей направлений деятельности, ведущих специалистов;

схемы движения документов

круг лиц, составляющих, визирующих, подписывающих конфиденциальные документы

состав конфиденциальных документов, получаемых от других организаций

состав конфиденциальных документов, составляемых по системам документации

практика составления и схемы движения каждого конфиденциального документа

организация хранения и уничтожения конфиденциальных документов

формы проверки наличия документов

Литература

Делопроизводство. Более 120 документов. М.: Проспект, 2003

Степанов Е.А. Информационная безопасность и защита информации : Учеб. пособие для вузов. – М. : Инфра-М, 2004

Занятие 5-6.

Цель – определить содержание перечня конфиденциальных сведений

Задание.

Составить перечень конфиденциальных документов фирмы по указанию преподавателя, расположив документы по тематическим группам или по структурным подразделениям и ранжировав их по степени значимости. Оформить гриф утверждения и визы согласования.

п.п	Наименование документов	Гриф конфиденциальности	Срок конфиденциальности

Источники

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»

Литература

Делопроизводство. Более 120 документов. М.: Проспект, 2003

Степанов Е.А. Информационная безопасность и защита информации : Учеб. пособие для вузов. – М. : Инфра-М, 2001

Занятие 7.

Цель – определить содержание основополагающих документов службы безопасности.

Задание.

1. Составить положение о службе безопасности фирмы
2. Оформить таблицу о структуре службы безопасности, разбив ее по функциональным группам.

Группы СБ, должности	Количество штатных единиц	Образование, опыт работы	Функции

Литература

Одинцов А.А. Служба безопасности на предприятии. М., 1995.

Ярочкин В.И. Система безопасности фирмы. М., 1997.

Ярочкин В.И. Служба безопасности коммерческого предприятия: Организационные вопросы. М., 1995.

Крысин А.В. Безопасность предпринимательской деятельности. М., 1996.

Левин А.В. Секрет фирмы. М., 1992.

Занятие 8.

Цель – определить оптимальный маршрут движения конфиденциального документа от момента создания или регистрации до передачи на архивное хранение или уничтожения; выявить круг лиц, могущих иметь доступ к конфиденциальному документу при его прохождении по организации.

Задание.

1. Составить графические схемы движения поступившего и изданного конфиденциальных нескольких видов документов по указанию преподавателя.

2. Определить алгоритм регистрации и учета конфиденциального документа по указанию преподавателя.

Литература

Делопроизводство. Более 120 документов. М.: Проспект, 2003

Алексенцев А.И. Конфиденциальное делопроизводство. М.: ООО «Журнал Управление персоналом», 2005

Степанов Е.А. Информационная безопасность и защита информации : Учеб. пособие для вузов. – М. : Инфра-М, 2004

Занятие 9-10.

Цель – сформировать пакет документов, возникающих при оформлении допуска сотрудника к конфиденциальной информации.

Задание.

1. Составить текст дополнения к трудовому договору, должностную инструкцию и обязательство о сохранении коммерческой тайны для сотрудника, получившего допуск к конфиденциальной информации фирмы.

2. Составить текст дополнений в правила внутреннего трудового распорядка фирмы, относительно необходимости сохранять коммерческую тайну.

Литература

Делопроизводство. Более 120 документов. М.: Проспект, 2003

Алексенцев А.И. Конфиденциальное делопроизводство. М.: ООО «Журнал Управление персоналом», 2005

Степанов Е.А. Информационная безопасность и защита информации : Учеб. пособие для вузов. – М. : Инфра-М, 2004

Занятие 11-12.

Цель – по журналам и карточкам учета построить поисковую систему конфиденциальных документов.

Задание.

Зарегистрировать в соответствующих журналах (карточках) учета по указанию преподавателя:

поступившие конфиденциальные пакеты и документы,
изданные документы,

носители конфиденциальной информации,
документы, определенные на выделенное хранение,
документы, предназначенные для копирования и тиражирования.

Литература

Алексенцев А.И. Конфиденциальное делопроизводство. М.: ООО «Журнал Управление персоналом», 2005

Занятие 13.

Цель – обобщить требования, предъявляемые на разных стадиях работы с конфиденциальными документами.

Задание.

Составить памятку по работе с конфиденциальными документами с учетом требований

по приему и первичной обработке документов
при передаче документов исполнителям
работе исполнителей с черновиками документов
при систематизации документов в дела
при копировании и тиражировании документов
при проверке наличия конфиденциальных документов

Литература

Делопроизводство. Более 120 документов. М.: Проспект, 2003

Алексенцев А.И. Конфиденциальное делопроизводство. М.: ООО «Журнал Управление персоналом», 2003

Занятие 14.

Цель – определить возможные инженерно-технические средства для защиты носителей конфиденциальной информации.

Задание.

По предложенным преподавателем планам офисных помещений определить:

предназначение кабинетов,
помещение для хранения конфиденциальных документов;
помещение для проведения конфиденциальных переговоров;
размещение камер видеонаблюдения.

Литература

Алексенцев А.И. Конфиденциальное делопроизводство. М.: ООО «Журнал Управление персоналом», 2003

Занятие 15-16.

Цель – выявить направления защиты информации в условиях функционирования на предприятиях и в организациях электронного документооборота, а также при использовании в управлении информационных сетей.

Задание.

На основании материалов интернет-ресурсов определить возможности защиты информации при работе автоматизированных систем электронного документооборота «Евфрат», «OfficeMedia», «CompanyMedia», «Босс-референт», «Галактика», «Директум» и составить сравнительную таблицу сделанных выводов, расположив программные продукты по рейтинговой системе.

ТЕМЫ РЕФЕРАТОВ

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
5. Правовые основы защиты конфиденциальной информации.
6. Экономические основы защиты конфиденциальной информации.
7. Организационные основы защиты конфиденциальной информации.
8. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
9. Составление инструкции по обработке и хранению конфиденциальных документов.
10. Направления и методы защиты документов на бумажных носителях.
11. Направления и методы защиты машиночитаемых документов.
12. Организация оперативного и архивного хранения конфиденциальных документов.
13. Порядок подбора персонала для работы с конфиденциальной информацией.
14. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
15. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
16. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
17. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
18. Порядок защиты информации в рекламной и выставочной деятельности.
19. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
20. Анализ источников, каналов распространения и каналов утечки информации.
21. Персонал как основной канал утечки конфиденциальной информации.
22. Назначение, виды, структура и технология функционирования системы защиты информации.
23. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
24. Аналитическая работа по выявлению каналов утечки информации фирмы.
25. Государственная тайна и порядок ее защиты.

26. Организация защиты авторских и смежных прав в РФ.
27. Направления и методы защиты профессиональной тайны.
28. Нотариальная тайна и порядок ее защиты.
29. Адвокатская тайна и порядок ее защиты.
30. Тайна страхования и порядок ее защиты.
31. Банковская тайна и порядок ее защиты.
32. Тайна почтовых отправлений и порядок ее защиты.
33. Направления и методы защиты служебной тайны.
34. Направления и методы защиты персональных данных о гражданах.
35. Методы защиты личной и семейной тайны.
36. Построение и функционирование защищенного документооборота.
37. Учет поступающей и отправляемой конфиденциальной корреспонденции.
38. Организация учета изданных конфиденциальных документов, их уничтожение.
39. Защита секретов в дореволюционной России.
40. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.
41. Организация проверок наличия конфиденциальных документов.
42. Порядок формирования и оформления конфиденциальных дел.
43. Создание и функции службы безопасности на предприятии.

ВОПРОСЫ К ЭКЗАМЕНУ

1. Основные законодательные акты в области информационной безопасности.
2. Виды и состав угроз информационной безопасности.
3. Понятие тайны, секрета. Виды тайны.
4. Понятие конфиденциального документа, сроки ограничения доступа к документу.
5. Законодательное регулирование защиты государственной тайны.
6. Содержание служебной тайны.
7. Содержание и направления защиты адвокатской тайны
8. Содержание и направления защиты нотариальной тайны
9. Содержание и направления защиты журналистской тайны
10. Содержание и направления защиты банковской тайны
11. Содержание и направления защиты тайны страхования.
12. Содержание и направления защиты коммерческой тайны.
13. Содержание личной и семейной тайны, персональные данные о гражданах.
14. Источники конфиденциальной информации и каналы ее объективного распространения.
15. Состав источника конфиденциальной информации – персонала фирмы.
16. Состав источника конфиденциальной информации – документации фирмы.
17. Виды угроз источникам и каналам распространения конфиденциальной информации.
18. Понятие и условия возникновения угроз конфиденциальной информации.
19. Состав основных угроз конфиденциальным традиционным и электронным документам.
20. Организационные каналы утраты конфиденциальной информации.
21. Технические каналы утраты конфиденциальной информации.
22. Содержание аналитической работы по выявлению каналов утраты конфиденциальной информации.
23. Основные направления и методы проверки наличия документов, дел и баз данных.
24. Понятие системы защиты информации, ее место в информационной безопасности фирмы.
25. Содержание элемента правовой защиты информации.
26. Содержание элемента организационной защиты информации.
27. Содержание элементов программно-аппаратной и криптографической защиты информации.

28. Состав и содержание ценной информации фирмы, подлежащей защите.

29. Назначение, порядок разработки и ведения перечня сведений, составляющих тайну фирмы, назначение перечня конфиденциальных документов.

30. Порядок приема или перевода сотрудников на работу, связанную с владением конфиденциальной информацией.

31. Понятие, назначение и содержание разрешительной (разграничительной) системы доступа персонала фирмы к конфиденциальной информации. Иерархичность доступа персонала к электронным документам.

32. Назначение и структура текущей работы с персоналом, владеющим тайной фирмы. Порядок обучения и инструктирования сотрудников. Воспитательная работа с персоналом, владеющим конфиденциальной информацией.

33. Порядок увольнения сотрудников, владеющих конфиденциальной информацией.

34. Понятие и содержание защищенного документооборота. Документопотоки, характеристика стадий каждого документопотока.

35. Требования, предъявляемые к технологической системе обработки конфиденциальных документов, виды технологических систем.

36. Технология обработки поступивших и отправляемых конфиденциальных документов.

37. Учет конфиденциальных документов и учетных форм, построение справочно-информационного банка данных по документам.

38. Назначение и виды учета конфиденциальных документов.

39. Особенности автоматизированного учета конфиденциальных документов.

40. Порядок работы персонала с конфиденциальными традиционными и электронными документами.

41. Оформление, формирование, учет и хранение дел с конфиденциальными документами.

42. Защита конфиденциальной информации фирмы при проведении совещаний и переговоров, приеме посетителей.

43. Нормативно-методическое обеспечение защиты документированной информации. Состав дополнений, вносимых в организационные документы фирмы в целях построения системы защиты информации.

44. Порядок уничтожения конфиденциальных документов.

45. Порядок работы исполнителей с конфиденциальными документами.

46. Порядок изготовления, копирования и тиражирования конфиденциальных документов.

47. Особенности документирования конфиденциальной информации.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ ПО ВСЕМУ КУРСУ

- Конституция РФ 1993 г.
Гражданский кодекс РФ 1994, 1995 г.
Кодекс РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ (в ред. от 26.07.2004)
Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ (в ред. 27.04.2004)
Уголовный кодекс РФ от 13.06.96 № 63-ФЗ (в ред. от 08.12.2003)
Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Федеральный закон от 03.04.95 № 40-ФЗ «О федеральной службе безопасности в Российской Федерации».
Федеральный закон от 12.08.95 № 144-ФЗ «Об оперативно-розыскной деятельности».
Федеральный закон от 31.05.96 № 61-ФЗ «Об обороне» (в ред. от 22.08.2004)
Федеральный закон от 10.01.96 № 5-ФЗ «О внешней разведке» (в ред. от 22.08.2004).
Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (в ред. от 22.08.2004)
Закон РФ от 05.03.92 № 2446-1 «О безопасности» (в ред. от 25.07.2002).
Закон РФ от 21.07.93 « 5485-1 «О государственной тайне» (в ред. от 29.06.2004).
Закон РФ от 11.02.92 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» (в ред. от 10.01.2003).
Закон РФ от 27.12.91 « 2124-1 «О средствах массовой информации» (в ред. от 22.08.2004)
Патентный закон РФ от 23.09.92 « 3517-1 (в ред. от 07.02.2003).
Закон РФ от 09.07.93 № 5351-1 «Об авторском праве и смежных правах» (в ред. от 20.07.2004).
Закон РФ от 23.09.92 № 3526-1 «О правовой охране топологий интегральных микросхем» (в ред. от 09.07.2002).
Указ Президента РФ от 10.01.2000 № 24 «О Концепции национальной безопасности Российской Федерации».
Указ Президента РФ от 30.11.95 № 1203 «О перечне сведений, отнесенных к государственной тайне» (в ред. от 29.05.2002).
Указ Президента РФ от 20.01.94 № 170 «Об основах государственной политики в сфере информатизации» (в ред. от 09.07.97).
Указ Президента РФ от 31.12.93 № 2334 «О дополнительных гарантиях прав граждан на информацию» (в ред. от 01.09.2000).
Указ Президента РФ от 08.11.95 № 1108 «О Межведомственной комиссии по защите государственной тайны»

- Ярочкин В.И. Информационная безопасность: Учебник для студ. вузов. – М. : Международные отношения, 2000
- Зегжда Д.П. Основы безопасности информационных систем : Учеб.пособие для вузов . – М. : Горячая линия-Телеком, 2000
- Степанов Е.А. Информационная безопасность и защита информации : Учеб. пособие для вузов. – М. : Инфра-М, 2001
- Алексенцев А.И. Конфиденциальное делопроизводство. М.: ООО «Журнал Управление персоналом», 2003
- Гаценко О.Ю. Защита информации: Основы организационного управления. – СПб. : Сентябрь, 2001
- Бачило И.Л. Информационное право : Учебник для вузов / Под ред. Топорнина Б.Н.;РАН. Ин-т государства и права. – СПб. : Юридический центр Пресс, 2001
- Галатенко В.А. Основы информационной безопасности : Курс лекций. М. : ИНТУИТ. РУ Интернет-Университет, 2003
- Галатенко В. А. Стандарты информационной безопасности : Курс лекций для вузов. – М. : Интернет-университет информационных технологий, 2004 .
- Партыка Т.Л. Информационная безопасность : Учебное пособие – М. : ФОРУМ-ИНФРА-М, 2004
- Степанова Е.Е. Информационное обеспечение управленческой деятельности : Учебное пособие для учреждений сред. проф. образования. – М. : Форум : Инфра-М, 2004
- Конеев И.Р. Информационная безопасность предприятия – СПб : БХВ-Петербург, 2003
- Шиверский А.А. Защита информации. Проблемы теории и практики. М.: Юрист, 1996.
- Герасименко В.А., Малюк А.А. Основы защиты информации. М.: ООО «Инкомбук», 1997
- Бержье Ж. Промышленный шпионаж на службе монополий. М., 1986.
- Герасименко В.А. Защита информации в автоматизированных системах обработки данных. М., 1994.
- Герасименко В.А., Гришаев С.П., Павлов Д.В: и др. Основы защиты коммерческой информации и интеллектуальной собственности. М., 1991.
- Киселев А.Е., Чаплыгин В.М., Шейкин М.С. Коммерческая безопасность. М., 1993.
- Копылов В.А. Информационное право: Учеб. пособие. М., 1997.
- Концепция информационной безопасности России / Под ред. Д.С. Черешкина. М., 1994.
- Крысин А.В. Безопасность предпринимательской деятельности. М., 1996.
- Левин А.В. Секрет фирмы. М., 1992.

Мельников В. Защита информации в компьютерных системах. М., 1997.

Ярочкин В.И. Коммерческая информация фирмы: Утечка или разглашение конфиденциальной информации? М., 1997.

Ярочкин В.И. Безопасность информационных систем. М., 1996.

Ярочкин В.И., Шевцова Г.А. Словарь терминов и определений по безопасности информации. М., 1996.

Печатается в авторской редакции
Компьютерная верстка, макет В.И. Никонов

Подписано в печать 25.10.06

Гарнитура Times New Roman. Формат 60x84/16. Бумага офсетная. Печать оперативная.

Усл.-печ. л. 1,5. Уч.-изд. л. 0,87. Тираж 100 экз. Заказ № 548

Издательство «Универс групп», 443011, Самара, ул. Академика Павлова, 1

Отпечатано ООО «Универс групп»